

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the U.S. Patent Application of

Thomas BREITBACH et al. Examiner: Lu, Zhyu

Serial No.: 09/936,834 Art Unit: 2618

Date Filed: September 17, 2001 Docket No.: P-44 MG

Confirmation No.: 1508

Title: Method for Using Standardized Bank Services via the Internet

Commissioner of Patents

P.O. Box 1450

Alexandria, VA 22313-1450

RULE 131 DECLARATION

Sir:

This declaration is submitted to establish a date of invention of the subject matter of the rejected claims in a WTO member country prior to the March 2, 1999 publication of Version 2.1 of "HBCI HOMEBANKING COMPUTER INTERFACE - Interface Specification" that is applied in the rejection of the claims in the Office Action dated September 7, 2007. To establish such date of invention, I submit the following documents as evidence:

1) a true and correct photocopy of a report of invention, the exact date of which is January 14, 1999 which is prior to March 2, 1999; and

2) a true and correct photocopy of correspondence showing that the report of invention was forwarded to my patent attorney, Dr.-Ing. Peter Riebling, prior to March 2, 1999.

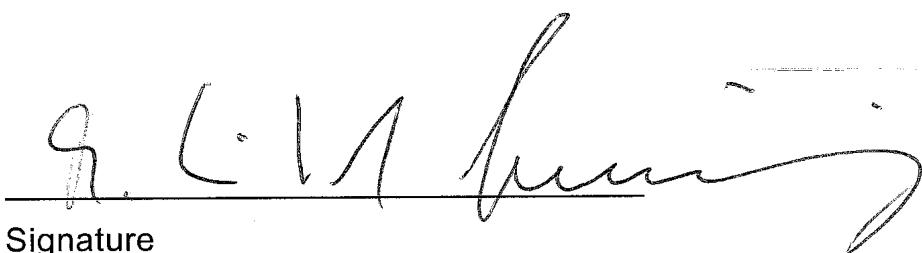
On the date of the report of invention, I was an employee of the assignee, T-Mobile Deutschland GmbH (former DeTeMobil Deutsche Telekom MobilNet GmbH), and my office was located in Germany. Dr.-Ing. Peter Riebling was a patent attorney hired by the assignee to prepare and file a patent application for the invention. His office was located in Germany. The submitted documents show that the report of invention existed and was forwarded to the patent attorney prior to March 2, 1999. The sending and receiving of these documents occurred in Germany, which is a WTO country.

From these documents, it can be seen that the date of invention of the claimed subject matter is before the March 2, 1999 publication date of the HBCI Specification document.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name: Dr. Richard Sinnig

Title: Head of Patent Department of T-Mobile Deutschland GmbH (in 1999)


Signature

Date: November 21, 2007

• • • T - Mobil -

Telefax

Empfänger Patentanwalt Dr.-Ing. Peter Riebling

Bitte
weiterleiten an

Ihre
Telefaxnummer 08382-78027

Anzahl Seiten
(inkl. Deckblatt) 2

Ansprechpartner Cécile Leloup (Sachgebiet Patente komm.), T214

Direkt Telefon: 0228/936-1229, Telefax: 0228/936-2225

Datum 1. Februar 1999

Thema Auftrag

Unser Zeichen: T99002 DE

Vorlage	Ablage	1/1506
Haupttermin		
Eing.:	02.FEB.1999	
PA.	Dr. Peter Riebling	
Bearb.:		Vorgelegt.

Herr Stoszki

Sehr geehrter Herr Dr. Riebling,

hiermit übersenden wir Ihnen eine weitere Erfindung aus unserem Hause
zur Ausarbeitung von Unterlagen für eine Patentanmeldung!

Arbeitsstitel:

„Standardisierte Bankdienstleistungen über Mobilfunk“.

Sie erreichen die Erfinder:

- 1.) Hrn. Dr. Breitbach telefonisch unter 0228/936-3315 (Fax: -3398)
- 2.) Hrn. Conrad unter 0228/936-2712 (Fax: -882712) und
- 3.) Hrn. Dr. Maringer unter 0228/936-1249 (Fax: -3309).

Mit freundlichen Grüßen

DeTeMobil
Deutsche Telekom MobilNet GmbH
-Abteilung Patente/Marken/Lizenzen-

i.A.


Dr. Richard Sinnig

i.A.


Cécile Leloup

Anlagen

Unterlagen der Erfindung

Stand der Technik

HBCI (Home Banking Computer Interface) ist ein von der deutschen Kreditwirtschaft entwickeltes Verfahren zum bankenübergreifenden Homebanking durch den Einsatz z.B. von einem Personal Computer (PC) und einem Festnetzmodem.

Angabe der Vorteile der Erfindung gegenüber dem Stand der Technik

Die Erfindung erlaubt es, neben dem Heimcomputer auch Mobiltelefone ohne Zusatzgeräte als kundenseitige HBCI-Plattform einzusetzen.

Genaue und ausführliche Beschreibung der Wirkungsweise der Erfindung

HBCI beruht auf einer kryptographischen Ende-zu-Ende Sicherung zwischen einer Chipkarte bzw. Diskette auf Kundensystemseite und dem Bankserver. Grundlage dieser Erfindung ist die Verteilung des kundenseitigen HBCI-Systems auf zwei Komponenten - die GSM-SIM-Karte und einen HBCI-Gateway. Ein direkter Einsatz des HBCI-Protokolls bis zur GSM-SIM-Karte verbietet sich sowohl aus Kapazitätsgründen, als auch wegen der sitzungsorientierten Ausrichtung des HBCI-Protokolls. Es werden zwei Übertragungsstrecken zwischen SIM-Karte und HBCI-Gateway und zwischen HBCI-Gateway und Bankserver gebildet. Auf beiden Strecken wird eine kryptographische Sicherung realisiert.

Der HBCI-Gateway wird in den Übermittlungsweg eingefügt. Dieser entpackt das HBCI-Protokoll, wandelt den Protokollablauf derart, daß eine Vereinbarkeit mit der GSM-SIM-Karte (mit z.B. dem Short Message Service bzw. GPRS als Trägerdienst) erwirkt wird. Der HBCI-Gateway schließlich tauscht das gewandelte Protokoll mit einer kundenseitig verwendeten SIM-Karte aus. Aus Sicht des Bankenservers wird komplett ein standardkonformes HBCI-Protokoll genutzt; zwischen Bankserver und HBCI-Gateway findet die durch HBCI definierte Sicherheit Anwendung. Zwischen HBCI-Gateway und SIM-Karte wird ein neues Sicherheitsprotokoll verwendet. Dieses entspricht einem vom Datenumfang her reduzierten, aber sicherheitstechnisch HBCI äquivalenten Protokoll.

Zusätzlich zeichnet sich die Erfindung dadurch aus, daß ein Verfahren zur Anwendung kommt, welches ermöglicht, kryptographische Schlüssel nach der SIM-Kartenpersonalisierung sicher in der SIM-Karte zu generieren und zu speichern. Hierzu wird vom HBCI-Gateway ein spezieller PIN-Brief erzeugt. Die Eingabe der PIN am Mobiltelefon generiert den kundenspezifischen Schlüssel in der SIM-Karte. Auf diese Weise wird ein sicherer, verschlüsselter Kommunikationsweg zwischen HBCI-Gateway und SIM-Karte ohne Gefährdung durch „man in the middle“ Attacken (z.B. den Netzwerkbetreiber) aufgebaut.

T99002 Erf

Telefax

• • • T • • Mobil •



00001572

Empfänger T214
 Bitte weiterleiten an Dr. Sinning
 Ihre Telefaxnummer -2225
 Anzahl Seiten (inkl. Deckblatt) 6

Ansprechpartner Dr. Thomas Breitbach, Systemsicherheit

Direkt Telefon: 0228/936-3315, Telefax: 0228/936-3398

Datum 14. Januar 1999

Thema Erfindungsmeldung

T • • Mobil •

14. JAN. 1999

tel. Abteilung
 Patente/Marken/Lizenzen

Sehr geehrter Herr Sinning,

anbei finden Sie eine Erfindungsmeldung zum Thema Mobilfunkbanking.

Herr Maringer hatte mit Ihnen die Thematik bereits kurz erörtert. Die Erfindungsmeldung der anderen Beteiligten werden nachgereicht.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mfg

Thomas Breitbach

Hausanschrift
 Postanschrift
 Telekontakte
 Aufsichtsrat
 Geschäftsführung
 Generalbev.
 Bankverbindung
 Eintrag
 Umsatzsteuer Nr.

DeTeMobil Deutsche Telekom MobilNet GmbH
 Landgrabenweg 151, 53227 Bonn
 Postfach 300463, 53184 Bonn
 Telefon: (0228) 936-0, Telefax: (0228) 936-9360, Internet: www.T-Mobil.de
 Dr. Ron Sommer (Vors.)
 Kai-Uwe Riecke (Vors.), Michael Günther, Reinhard Holzkamp, Klaus Hummel, Holger Kranzusch, René Obermann
 Roland Mahler
 Dresdner Bank Bonn, Konto Nr. 2 062 240 00, BLZ 370 800 40, Postbank AG Essen, Konto Nr. 10090-437, BLZ 360 100 43
 Amtsgericht Bonn, HRB 59 19
 DE 122265872



Erfindungsmeldung/ -mitteilung

(Pro Erfinder ist eine Erfindungsmeldung/-mitteilung auszufüllen)

!!! Jedes außerbetriebliche Bekanntwerden einer Erfindung vor Anmeldung führt zum Verlust der Schutzhaltbarkeit !!!**Als Eingang der Erfindungsmeldung/-mitteilung gilt nur der Eingang in der Abteilung Patente/Marken/Lizenzen****DeTeMobil Deutsche Telekom MobilNet GmbH, Landgrabenweg 151, 53227 Bonn****Persönliche
Angaben**

Name:	Breitbach	Personalnummer:	323179
Vorname:	Thomas	Stellenbezeichnung:	T211
Akademischer Titel:	Dr.	Firmaninterne Position:	SB
Telefon:	0228/936-3315	Telefax:	0228/936-3398
Zuständigkeitsbereich:	System Sicherheit	Staatsangehörigkeit:	deutsch
Beteiligung an der Erfindung (in %):	33,33		
Privatanschrift:	Kolpingstr. 23a, 56645 Nickenich		

Ich melde
folgende Erfahrung**1. Bezeichnung der Erfindung:****Standardisierte Bankdienstleistungen über Mobilfunk****2. Erfinder**

Name:	Maringer	Personalnummer:	31125
Vorname:	Günther	Stellenbezeichnung:	T243
Akademischer Titel:	Dr.	Firmaninterne Position:	FL
Telefon:	0228/936-1249	Telefax:	0228/936-3309
Zuständigkeitsbereich:	Chipkartensysteme	Staatsangehörigkeit:	deutsch
Beteiligung an der Erfindung (in %):	33,33		
Privatanschrift:	Troschelstr. 8, 53115 Bonn		

3. Erfinder

Name:	Conrad	Personalnummer:	30122
Vorname:	Alan	Stellenbezeichnung:	M221
Akademischer Titel:		Firmaninterne Position:	SB
Telefon:	0228/936-2712	Telefax:	0228/936-882712
Zuständigkeitsbereich:	Produktmanagement	Staatsangehörigkeit:	UK
Beteiligung an der Erfindung (in %):	33,33		
Privatanschrift:	Freie Bitze 24, 53639 Königswinter		



Name: Thomas Breitbach

Erfindungsmeldung/ mitteilung

(Pro Erfinder ist eine Erfindungsmeldung/ mitteilung auszufüllen)

3. An der Erfindung sind folgende Firmenfremde beteiligt:

Name, Firma

4. Der Erfindung liegt folgende Aufgabe zugrunde (Problem):

Derzeit bietet der HBCI-Standard der deutschen Kreditwirtschaft die Möglichkeit, Homebanking über einen bankenübergreifenden Standard anzubieten. Die Erfindung schlägt ein Konzept vor, diese Dienste auch über ein GSM-Mobiltelefon anzubieten.

5. Die Erfindung wird als dienstgebunden betrachtet (§4 ArbEG), d.h.:

daß die Erfindung während der Dauer des Arbeitsverhältnisses gemacht wurde und entweder

die Erfindung aus dem Zuständigkeitsbereich des Arbeitnehmers entstanden ist oder

die Erfindung maßgeblich auf Erfahrungen oder Arbeiten des Betriebes beruht.

Die Erfindung wird als nicht dienstgebunden betrachtet (§18, 19 ArbEG):

6. Veröffentlichungen der Erfindung sind beabsichtigt

a) nein Vorläufig nichtb) als druckschriftliche Veröffentlichung

Name des Publikationsorgans:

Erscheinungsdatum:

c) Veröffentlichung durch Vortrag

Ort der Veranstaltung:

Datum der Veranstaltung:

7. An Unterlagen für die Ausarbeitung einer Schutzrechtsanmeldung sind beigefügt
(soweit möglich bitte nur 1 Exemplar für die Erfinder gemeinsam):

a) Schilderung des Standes der Technik mit Fundstellenangabe

b) Angabe der Vorteile der Erfindung gegenüber dem Stand der Technik

c) Genaue und ausführliche Beschreibung der Wirkungsweise der Erfindung

d) Handskizzen, Schaltbilder, Zeichnungen

e) ggf. Meßprotokolle, technische Berichte



Name: Thomas Breitbach

Erfindungsmeldung/ -mitteilung

(Pro Erfinder ist eine Erfindungsmeldung/-mitteilung auszufüllen)

8. Entstehung der Erfindung:
 Ich bin zu der Erfindung veranlaßt worden:

- a) weil der Arbeitgeber eine Aufgabe gestellt hat unter Angabe des Lösungsweges
- b) weil der Arbeitgeber eine Aufgabe gestellt hat ohne Angabe des Lösungsweges
- c) ohne daß der Arbeitgeber eine Aufgabe gestellt hat, jedoch durch die infolge der Firmenzugehörigkeit erlangte Kenntnis von Mängeln und Bedürfnissen, die nicht selbst festgestellt wurden
- d) ohne daß der Arbeitgeber eine Aufgabe gestellt hat, jedoch durch die infolge der Firmenzugehörigkeit erlangte Kenntnis von Mängeln und Bedürfnissen, die selbst festgestellt wurden
- e) weil ich mir/wir uns innerhalb meines/unseres Aufgabenbereiches eine Aufgabe gestellt habe(n)
- f) weil ich mir/wir uns außerhalb meines/unseres Aufgabenbereiches eine Aufgabe gestellt habe(n)

9. Lösung der Aufgabe (Mehrfachnennungen möglich):

- a) Die Lösung wurde mit Hilfe beruflich geläufiger Überlegungen gefunden
- b) Die Lösung wurde aufgrund Arbeiten oder Erfahrungen des Arbeitgebers gefunden
- c) Technische Hilfsmittel des Arbeitgebers wurden benutzt

10. Die Erfindung wurde als Verbesserungsvorschlag eingereicht nein ja, falls bekannt bitte VwG-Nr. angeben:

Ich versichere, daß keine weiteren Personen als hier aufgeführt am Zustandekommen der Erfindung beteiligt sind und daß mir keine Vorbenutzung/-veröffentlichung der Erfindung bekannt ist.

Ort, Datum	14.1.95 Bonn
Unterschrift des Erfinders	Thomas Breitbach

Stand der Technik

HBCI (Home Banking Computer Interface) ist ein von der deutschen Kreditwirtschaft entwickeltes Verfahren zum bankenübergreifenden Homebanking durch den Einsatz z.B. von einem Personal Computer (PC) und einem Festnetzmodem.

Angabe der Vorteile der Erfindung gegenüber dem Stand der Technik

Die Erfindung erlaubt es, neben dem Heimcomputer auch Mobiltelefone ohne Zusatzgeräte als kundenseitige HBCI-Plattform einzusetzen.

Genaue und ausführliche Beschreibung der Wirkungsweise der Erfindung

HBCI beruht auf einer kryptographischen Ende-zu-Ende Sicherung zwischen einer Chipkarte bzw. Diskette auf Kundensystemseite und dem Bankserver. Grundlage dieser Erfindung ist die Verteilung des kundenseitigen HBCI-Systems auf zwei Komponenten - die GSM-SIM-Karte und einen HBCI-Gateway. Ein direkter Einsatz des HBCI-Protokolls bis zur GSM-SIM-Karte verbietet sich sowohl aus Kapazitätsgründen, als auch wegen der sessionorientierten Ausrichtung des HBCI-Protokolls. Es werden zwei Übertragungsstrecken zwischen SIM-Karte und HBCI-Gateway und zwischen HBCI-Gateway und Bankserver gebildet. Auf beiden Strecken wird eine kryptographische Sicherung realisiert.

Der HBCI-Gateway wird in den Übermittlungsweg eingefügt. Dieser entpackt das HBCI-Protokoll, wandelt den Protokollablauf derart, daß eine Vereinbarkeit mit der GSM-SIM-Karte (mit z.B. dem Short Message Service bzw. GPRS als Trägerdienst) erwirkt wird. Der HBCI-Gateway schließlich tauscht das gewandelte Protokoll mit einer kundenseitig verwendeten SIM-Karte aus. Aus Sicht des Bankenservers wird komplett ein standardkonformes HBCI-Protokoll genutzt: zwischen Bankserver und HBCI-Gateway findet die durch HBCI definierte Sicherheit Anwendung. Zwischen HBCI-Gateway und SIM-Karte wird ein neues Sicherheitsprotokoll verwendet. Dieses entspricht einem vom Datenumfang her reduzierten, aber sicherheitstechnisch HBCI äquivalenten Protokoll.

Zusätzlich zeichnet sich die Erfindung dadurch aus, daß ein Verfahren zur Anwendung kommt, welches ermöglicht, kryptographische Schlüssel nach der SIM-Kartenpersonalisierung sicher in der SIM-Karte zu generieren und zu speichern. Hierzu wird vom HBCI-Gateway ein spezieller PIN-Brief erzeugt. Die Eingabe der PIN am Mobiltelefon generiert den kundenspezifischen Schlüssel in der SIM-Karte. Auf diese Weise wird ein sicherer, verschlüsselter Kommunikationsweg zwischen HBCI-Gateway und SIM-Karte ohne Gefährdung durch „man in the middle“ Attacken (z.B. den Netzwerkbetreiber) aufgebaut.

• • • T • • Mobil •

Telefax

Empfänger Kanzlei Riebling

Bitte weiterleiten an Herrn Stoinsky

Ihre Telefaxnummer 08382/8027

Anzahl Seiten (inkl. Deckblatt) 10

Ansprechpartner Dr. Günter Maringer, T2

Vorlage	Ablage	D1506
Haupttermin		
Eing.: 12.FEB.1999		
PA. Dr. Peter Riebling		
Bearb.:	Vorgelegt.	

Direkt Telefon: (0228) 936-1249, Telefax: (0228) 936-881249

Datum 12. Februar 1999

Thema „Standardisierte Bankdienstleistungen über Mobilfunk“

Sehr geehrter Herr Stoinsky,

in o.g. Angelegenheit hatten Sie um zusätzliche Informationen gebeten. Das beigefügte Papier erläutert die Konzepte im Detail.

Im Fall von Rückfragen stehe ich gern zur Verfügung.

Mit freundlichen Grüßen

DeTeMobil
Deutsche Telekom MobilNet GmbH



Er hat angerufen, undet sich nächste Woche?
G.M.

Hausanschrift DeTeMobil Deutsche Telekom MobilNet GmbH
Postanschrift Landgrabenweg 151, 53227 Bonn

Aufsichtsrat Postfach 300463, 53184 Bonn

Telefon: (0228) 936-0, Telefax: (0228) 936-9360, Internet: www.T-Mobil.de

Dr. Ron Sommer (Vors.)

Kai-Uwe Ricke (Vors.), Michael Günther, Reinhard Holekamp, Klaus Hummel, Holger Kranzusch, René Obermann

Roland Mahler

Geschäftsführung
Generaldirektor

ENTWURF

Technisches Konzept

Standardisierte Bankdienstleistungen über Mobilfunk

**Version 0.0.3
9. Februar 1999**

VERTRAULICH

...T...Mobil.

**Deutsche Telekom MobilNet GmbH
Landgrabenweg 151
D-53227 Bonn**

Phone: +49 228 936-0

© DeTeMobil Deutsche Telekom MobilNet GmbH 1999

Weitergabe oder Vervielfältigung dieser Unterlage, Verwertung oder Mitteilung ihres Inhalts oder dessen Speicherung auf Datenträgern jeder Art ist weder vollständig noch auszugsweise gestattet, soweit nicht ausdrücklich schriftlich zugestanden. Zu widerhandlungen verpflichten zu Schadenersatz. Alle Rechte vorbehalten.
(Schutzvermerk DeTeMobil GmbH)

Änderungshistorie

Version	Datum	Grund der Änderung
0.0.1	29.02.1999	Stichpunktsammlung, Thomas Breitbach
0.0.2	05.02.1999	Überarbeitung, Zusammenlegung des Dokumentes Thomas Breitbach, Günther Maringer
0.0.3	09.02.1999	Erster Review, Thomas Breitbach, Günther Maringer, Alan Conrad

1 EINFÜHRUNG	4
2 PRODUKTIDEE	4
3 INFRASTRUKTUR	6
4 SICHERHEIT	7

1 Einführung

Dieses Dokument beschreibt überblicksartig die Konzeption sicherer Bankdienstleistungen über GSM-Mobilfunk unter Verwendung des offenen HBCI-Standards. Die technischen Konzepte sollen im Rahmen einer Kooperation zwischen den Genossenschaftsbanken und T-Mobile umgesetzt werden.

Das vorliegende Dokument beschreibt zunächst grob die Produktidee sowie die Kundenprozesse. Einen Schwerpunkt des Dokumentes bildet das Sicherheitskonzept in Kapitel 4 sowie die Verteilung der benötigten kryptographischen Schlüssel.

2 Produktidee

Für die Inanspruchnahme von Bankdienstleistungen werden in zunehmendem Maß papierlose, bequeme Wege der Einreichung nachgefragt. Bankenseitig wird diese Entwicklung wegen der damit erzielbaren Rationalisierungseffekte gefördert. Die in Deutschland mit unter 10% recht geringe Penetration von PC-Online-Zugängen stellt hier allerdings zunächst ein Hemmnis dar.

Der Mobilfunk mit ca. 15 Millionen Kunden und hohen Wachstumsraten ist erheblich weiter verbreitet. Hier liegt ein möglicher Schlüssel für einen massenmarktfähigen elektronischen Zugang zu Banktransaktionen. Hinzu kommt für den Kunden die Möglichkeit, auch mobil Zugang zu Bankgeschäften zu erlangen. Anstelle des PC übernimmt hier die Chipkarte die Rolle des Client, sowohl was den Benutzerdialog, als auch was die Sicherheitsfunktionen angeht. Ermöglicht wird dies durch eine neue, standardisierte Technologie mit Namen SAT (SIM Application Toolkit), welcher es der Mobilfunk-Chipkarte (SIM-Karte) erlaubt, die Rolle der Dienststeuerung wahrzunehmen.

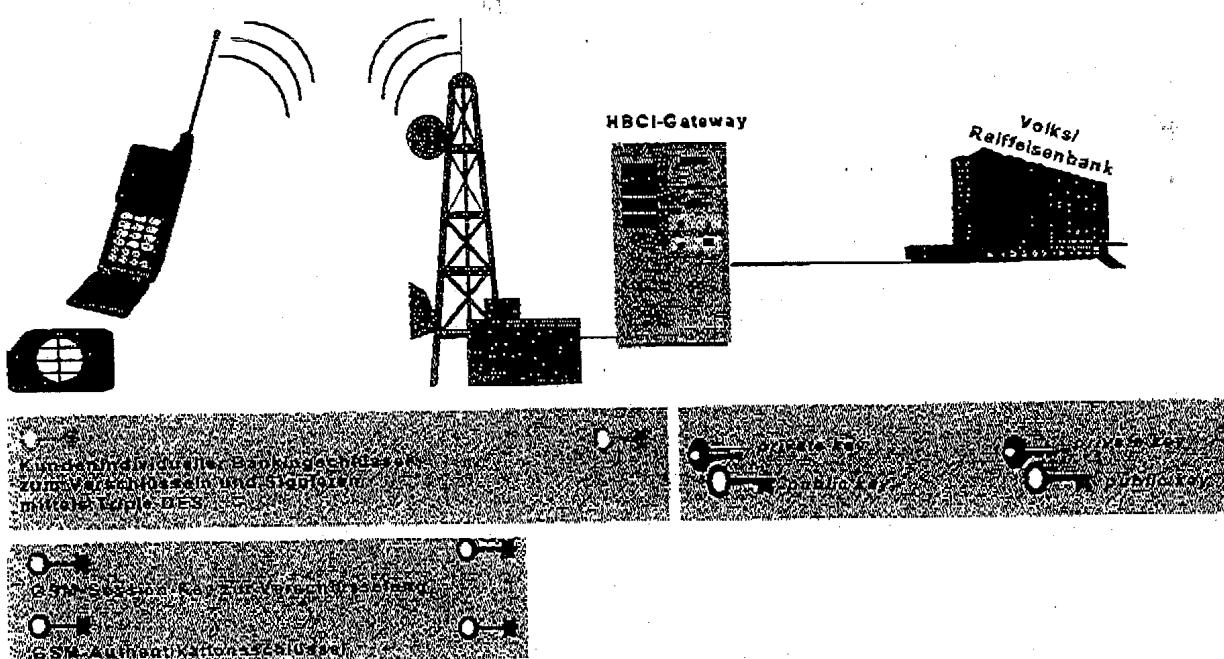
Der HBCI-Standard wird in der deutschen Bankenwelt die Plattform für Homebanking. Es liegt von daher nahe, auf diesen Standard auch im Kontext von mobilfunkgestütztem Banking aufzusetzen. Leider ist das für das Internet konzipierte HBCI-Protokoll zu umfangreich für eine direkte Abbildung auf die heutige GSM-Mobilfunkwelt. Dies betrifft sowohl die für die Datenübertragung notwendige Bandbreite, als auch die benötigte Speicherkapazität und Rechenleistung auf Client-Seite (SIM-Karte).

Von daher bietet sich ein Ansatz an, eine Transformation zwischen dem bankenseitig verwendeten HBCI und einem auf der Mobilfunkseite zu definierenden, komprimierten HBCI vorzunehmen. Aufgabe einer solchen transformierenden Komponente, im folgenden HBCI-Gateway genannt, ist die Reduktion der zu übertragenden Daten auf ein GSM-kompatibles Maß. Die Grundidee besteht also darin, daß sowohl die SIM-Karte als auch der Bankrechner jeweils direkt ausschließlich mit dem HBCI-Gateway kommuniziert, dieser also eine Proxy-Funktion wahrnimmt.

Diese Protokoll-Transformation wird als Evolutionsschritt auf dem Weg zu End-to-End HBCI angesehen. Es ist zu erwarten, daß die Bandbreite der Mobilfunknetze so wachsen wird, daß dies mittelfristig als realistisches Ziel erscheint.

Die erwähnte Transformation bringt auch eine Transformation der verwendeten Sicherheitsmechanismen mit sich; während zwischen dem Gateway und der Bankenwelt das HBCI-Protokoll angewendet wird, wird GSM-seitig ein eigenes Sicherheitsprotokoll verwendet. Der im folgenden unterbreitete Vorschlag basiert auf der RDH-Variante für HBCI und auf einer symmetrischen Triple-DES Lösung auf GSM-Seite.

Die folgende Figur veranschaulicht vereinfacht den Sachverhalt:



Auf der GSM-Luftschnittstelle kommt die GSM-Standardverschlüsselung zur Anwendung. Darüber liegt auf Applikationsebene eine Triple-DES Verschlüsselung, welche die Strecke zwischen SIM-Karte und HBCI-Gateway absichert. Die Strecke zwischen HBCI-Gateway und Bank unterliegt dem Standard-HBCI-Protokoll in der RDH-Variante.

Da der HBCI-Gateway sicherheitsrelevante Funktionen wahrnimmt, wird die Arbeitsannahme getroffen, daß er in den Bankrechenzentren betrieben wird.

Zur Sicherung der Strecke zwischen HBCI-Gateway und SIM-Karte ist es erforderlich, einen geheimen Schlüssel zwischen dem Gateway und der SIM-Karte zu definieren. Um die Geheimhaltung des Schlüssels absolut sicherzustellen, wird ein Verfahren vorgeschlagen, bei welchem die Bank per PIN-Brief eine Initialisierungs-PIN an den Kunden versendet, welchen der Kunde einmalig am Mobiltelefon eingibt. In der SIM sowie im HBCI-Gateway wird daraus mittels eines geeigneten Algorithmus der Schlüssel abgeleitet. Damit ist sichergestellt, daß Dritte keine Kenntnis dieses Schlüssels haben. In Kapitel 4 wird diese Sicherheitsphilosophie ausführlich dargestellt.

2.1 Geschäftsvorfälle

In einem ersten Schritt wird vorgeschlagen, die Geschäftsvorfälle Kontostandsabfrage, Letzte Umsätze und Überweisungsauftrag anzubieten.

2.2 Bedieneroberfläche

Sämtliche Aktionen werden vom Nutzer über die Bedienersteuerung des Mobiltelefons angestoßen. Hierzu wird von der SIM-Karte ein eigener Menüpunkt "Mobile Banking" eingestellt. Nach Anwahl dieses Punktes werden die Unterpunkte "Kontostand", "Umsätze", "Überweisung" und "Konfiguration" angeboten.

Die begrenzten Möglichkeiten einer Mobiltelefon-Tastatur verlangen nach einer optimierten Benutzerführung. Hierzu wird insbesondere die eigene Bankverbindung in der Karte abgelegt, sodaß diese nur einmalig eingegeben werden muß.

Hierbei sollte berücksichtigt werden, daß in zahlreichen Fällen Kunden bei einer Bank mehrere Konten unterhalten. Eine geeignete Auswahlmöglichkeit sollte angeboten werden.

Um sicherzustellen, daß Unbefugte nicht in die Lage versetzt werden, Banktransaktionen zu veranlassen, sollte bei jeder Transaktionsanforderung eine PIN abgefragt werden. Diese PIN wird lokal von der Karte verwaltet.

Kontostandsabfrage

Nach Anwahl dieses Menüpunktes:

- Abfrage Konto (Auswahl aus Liste)
- Abfrage PIN
- Kunde erhält den Kontostand.

Umsätze

Nach Anwahl dieses Menüpunktes:

- Abfrage Konto (Auswahl aus Liste)
- Abfrage PIN
- Kunde erhält die letzten Umsätze.

Überweisung

- Nach Anwahl dieses Menüpunktes:
- Abfrage Konto (Auswahl aus Liste)
- Abfrage Zielkonto-Nr.
- Abfrage Ziel-BLZ
- Abfrage Betrag
- Abfrage Verwendungszweck
- Abfrage PIN
- Kunde erhält Bestätigung per SMS.

Konfiguration

Nach Anwahl dieses Menüpunktes:

- SMS-Zieladresse des HBCI-Gateways
- Abfrage BLZ und eigene Konto-Nummern (maximal n Konten)
- Abfrage Initialisierungs-PIN (siehe oben, 20 stellig dezimal + eine Prüfziffer zur Erkennung von Eingabefehlern).
- Abfrage PIN

Anschließend werden die eingegebenen Daten in der Karte abgelegt. Weiterhin werden Menüpunkte "Anzeigen" und "Löschen" angeboten.

3 Protokolle

3.1.1 Subskription

Die Freischaltung des Banking-Dienstes erfolgt durch Anwahl eines Menüpunktes "Konfiguration" (s.o.), hierauf werden BLZ und Konto-Nummern der eigenen Konten abgefragt, sowie Initialisierungs-PIN und lokale PIN für die Bankanwendung. Die Daten der eigenen Bankverbindungen werden auf der Karte abgespeichert. Aus der Initialisierungs-PIN wird von der Karte ein Schlüssel Ksms zur Sicherung der Kommunikation zwischen HBCI-GSM-Gateway und SIM-Karte berechnet (siehe Kap. 4). Die Abfrage der lokalen (Karten-) PIN dient dem Schutz gegen unauthorisierte Subskriptionsversuche.
Nach der Berechnung von Ksms meldet die SIM-Karte dem HBCI-Gateway den Subskriptionswunsch. Hierauf erfolgt die lokale Schlüsselgenerierung am HBCI-

Gateway sowie der Erstdialog mit dem HBCI-Bankensystem. Ferner sendet der HBCI-Gateway eine Nachricht zur Karte, welche das Anpassen des Bankmenü-Titels und das vollständige Aktivieren der Applikation bewirkt.

3.2 Geschäftsvorfälle

Für die einzelnen Geschäftsvorfälle sind geeignete Nachrichtenformate zu definieren. In jedem Fall erfolgt eine Verschlüsselung der Nachrichten mit Ksms.

4 Sicherheit

Eine sehr wichtige Anforderung an das hier beschriebene Produkt ist die Sicherheit. Ziel des Sicherheitskonzeptes ist vor allem, einen Mißbrauch zu verhindern (Authentifikation des Kunden). Des Weiteren ist es wichtig, die Vertraulichkeit der übertragenen Daten zu gewährleisten (Verschlüsselung der Übertragung). Beide Anforderungen werden mittels kryptographischer Verfahren realisiert.

4.1 Rollenmodell

Grundsätzlich lassen sich bei diesem Konzept die folgenden Rollen identifizieren:

- (1) Kunde
- (2) Netzbetreiber
- (3) Betreiber des HBCI-Gateways
- (4) Betreiber des HBCI-Kreditinstitutssystems (Rechenzentrum der Bank)

Die Rollen (3) und (4) sollten aus Sicherheitsgründen über ein ausgeprägtes Vertrauensverhältnis verfügen. Der Betreiber des HBCI-Gateways ist prinzipiell in der Lage, Nachrichten abzuhören oder fälschlich aufzusetzen. Sinnvollerweise sollte der Betreiber des HBCI-Gateways daher aus dem Bankenumfeld stammen.

4.2 Sicherheitsbereiche

Die gesamte Strecke vom Mobiltelefon des Kunden bis zum HBCI-Server der Bank ist in zwei Sicherheitsbereiche aufgegliedert. Der erste Bereich erstreckt sich vom der SAT-SIM-Karte bis zum HBCI-Gateway. Die Strecke vom HBCI-Gateway zum Bankenserver bildet den zweiten Sicherheitsbereich.

4.3 Sicherheitsbereich 1: SAT-SIM zu HBCI-Gateway

Die Sicherheitsfunktionen dieses Bereiches werden im wesentlichen durch Vergabe und Verwendung eines speziellen Schlüssels Ksms bestimmt. Mit diesem 128 Bit langen Triple-DES Schlüssel werden alle zwischen SAT-SIM und HBCI-Gateway ausgetauschten Nachrichten verschlüsselt.

Der Ksms sichert die Verbindung von der SIM bis zum HBCI-Gateway. Der Ksms authentifiziert sowohl Kunde als auch das HBCI-Gateway und wird auch zur Verschlüsselung dieser Strecke verwendet. Der Ksms ist ein spezifischer Schlüssel der Bankenapplikation und bleibt dem Netzbetreiber verborgen. Um dies zu gewährleisten, wird folgendes Verfahren zur Erzeugung angewandt:

Bei der Kartenspersonalisierung wird vom Netzbetreiber zusammen mit der Bankenapplikation ein KIV, ein Masterkey, zur Erzeugung der kundenspezifischen Ksms auf alle Karten aufgebracht. Der Kunde erhält vor Subskription des Dienstes die Daten seiner Bank inklusive einer 20 stelligen PIN. Bei der Initialisierung der SAT-Applikation (online-Subskription) wird aus der PIN mit Hilfe des KIV der eigentliche Kundenschlüssel Ksms erzeugt (verschlüsseln der PIN, der Bankleitzahl und der Kontonummer per Triple-DES mit KIV als Schlüssel).

Zur Erzeugung des Ksms im HBCI-Gateway muß die PIN auch zum Gateway-Betreiber weitergereicht werden. Optional bietet sich die Erzeugung der PIN am HBCI-Gateway und die Weitergabe an die Bank an.

Die Authentifikation der beiden Rollen Kunde und HBCI-Gateway erfolgt durch Wissen über die schriftlich ausgetauschte PIN. Zwischen Netzbetreiber und HBCI-Gateway-Betreiber muß zusätzlich der Masterkey KIV ausgetauscht werden. Dieser Masterkey authentifiziert damit zusätzlich das HBCI-Gateway.

Optional kann darüber hinaus noch folgende eine zusätzliche Authentifikation des Kunden über die Kennung seines Mobilanschlusses erfolgen:

GSM-Verbindungen werden durch einen speziellen Schlüssel (Ki) gesichert (GSM 02.09). Es kann beim HBCI-Gateway die Auswertung der Calling-Line-Identification (CLI) der versendeten SAT-SIM erfolgen. Dazu muß die DI-Rufnummer des Kunden im HBCI-Gateway verwaltet werden.

4.4 Sicherheitsbereich 2: HBCI-Gateway zum Kreditinstitussystem

Auf der Schnittstelle vom HBCI-Gateway zur Bank kommt ein unmodifiziertes HBCI-Protokoll zur Anwendung. Bezuglich der Ausgestaltung dieser Schnittstelle siehe [HBCI2]. In der hier dargestellten Ausgestaltung kommt die RDH-Variante zum Einsatz.

Im Modell der HBCI-Spezifikation stellt das HBCI-Gateway das Kundensystem dar. Auf dem HBCI-Gateway sind die öffentlichen und privaten Signier- und Chiffrierschlüssel für jeden Kunden gespeichert.

Der Mechanismus der Authentifikation der öffentlichen Kunden- sowie Bankenschlüssel muß in einer vertraglichen Regelung zwischen Betreiber des HBCI-Gateways und dem Betreiber des Bankenservers erfolgen. Sollte kein implizites Vertrauensverhältnis zwischen diesen Parteien bestehen, können Initiale oder auch Zertifikate eingesetzt werden.

4.5 Übersicht über die verwendeten Schlüssel

Schlüssel	Verwendung	Generierung	Aufbewahrungsorte	Krypto-verfahren Schlüssellänge	Kenntnis durch	Bemerkung
Ki	GSM-Authentisierung Luftschnittstelle	Netzbetreiber bei Kartenpersonalisierung	SIM, Authentification Center Netzbetreiber	Proprietär symmetrisch 128 bit	Netzbetreiber	
Kc	GSM Verschlüsselung Luftschnittstelle	Netz + SIM bei Verbindungsaufbau	Mobiltelefon + GSM-Netz	A5 54 Bit	Netzbetreiber	
CKpub	HBCI public key (Verschlüsselung) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway Bank	RSA 768 Bit	Gateway-Betreiber, Bank	
CKpriv	HBCI private key (Verschlüsselung) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway	RSA 768 Bit	Gateway-Betreiber	
AKpub	HBCI public key (Authentifikation) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway, Bank	RSA 768 Bit	Gateway-Betreiber	
AKpriv	HBCI private key (Authentifikation) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway	RSA 768 Bit	Gateway-Betreiber	

CBpub	HBCI public key (Verschlüsselung) der Bank		Bank, HBCI-Gateway	RSA 768 Bit	Gateway-Betreiber, Bank	
CBpriv	HBCI private key (Verschlüsselung) der Bank		Bank	RSA 768 Bit	Bank	
ABpub	HBCI public key (Authentifikation) der Bank		Bank, HBCI-Gateway	RSA 768 Bit	Gateway-Betreiber, Bank	
ABpriv	HBCI private key (Authentifikation) der Bank		Bank	RSA 768 Bit	Bank	
KIV	Masterkey zur Generierung von Ksms	Netzbetreiber	SIM-Karte	Triple-DES (2-key) 128 Bit	SIM-Karte, HBCI-Gateway	Hilfschlüssel zur Erzeugung des Ksms mittels PIN Masterkey, identisch für alle Kunden
Ksms	Verschlüsselung und Authentifikation SAT-SIM zum Gateway	HBCI-Gateway vor Subskription sowie SAT-SIM bei Subskription	HBCI-Gateway, SAT-SIM	Triple-DES (2-key) 128 Bit	Gateway-Betreiber, indirekt auch Kunde	Ksms wird in der Karte nach Eingabe einer PIN erzeugt

4.6 Gesamtbetrachtung

Das vorliegende technische Konzept bietet ein hohes Sicherheitsniveau. Die beteiligten technischen Komponenten (SIM, Mobiltelefon, HBCI-Gateway) sind weitaus weniger anfällig gegen Mißbrauch als etwa ein Kunden-PC. Aus Sicht des Kunden wird mit dem vorliegenden technischen Konzept ein neuartiger Dienst angeboten, welcher mit einem hohen Sicherheitsstandard einhergeht.

5 Ausblick

Das hier beschriebene Konzept stellt einen möglichen Ausgangspunkt für Dienste aus dem gesamten Bereich des „Mobile Electronic Commerce“ dar. Mittel- und langfristig sind folgende Erweiterungen des Konzeptes möglich:

- Erweiterung um Push-Dienste, d.h. vom Kreditinstitut angestossene Mitteilungen oder Transaktionen
- Unterstützung eines zweiten Kartenslots (Dual Slot Mobiles), darauf aufbauend Anbindung der Geldkarte (Transaktionen und Ladevorgänge)

6 Referenzen

- [HBCI2] Homebanking-Computer-Interface, Schnittstellenspezifikation Version 2.0.1 vom 02.02.1998
Bundesverband deutscher Banken e.V., Deutscher Sparkassen- und Giroverband e.V., Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Verband öffentlicher Banken e.V. (Hrsg.)
- [GSM 02.09] European digital cellular telecommunications system(Phase 2); Security aspects; (GSM 02.09), European Telecommunications Standards Institute 1994